BUILDING USABLE PRIVACY TOOLS – Why it's not the user's fault.

Henry – CEO of Techlore *(techlore.tech)*

So you want to be private? Great! Just...

1. Obtain devices without any personal information, then install an operating system like Qubes.
2. Utilize Whonix for everything within Qubes.
3. Install an E2EE messenger and migrate all your contacts over.
4. Stop using email, because email is insecure.
5. Self-host everything.
6. Only use Tor Browser without Javascipt on all websites.
7. Stop using phone numbers in all situations.
8. Utilize full-disk encryption.
9. Stop using search engines and rely on bookmarking & memorizing URLs.
10. Only FOSS.
11. Etc.

Our Track Coach

(Not actually him)

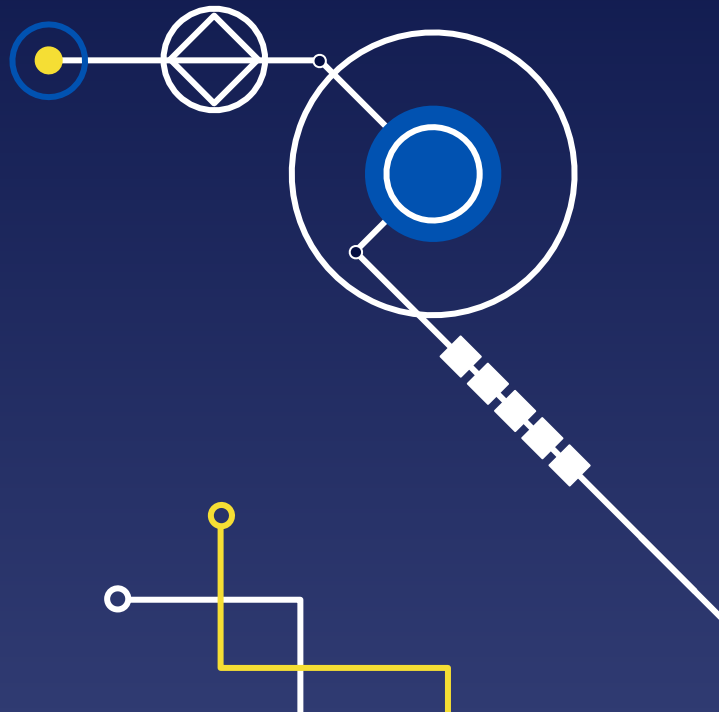
- Couldn’t figure out why his Apple watch kept buzzing.
- The digital efficacy of the average user is not as strong as you’d expect.
- The amount of time, energy, & education required to achieve higher degrees of privacy is too much.

How do we fix this problem?

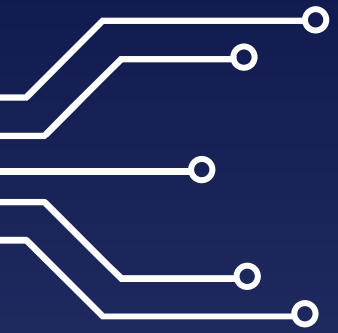
Solution 1 - We educate every user to make them more private.

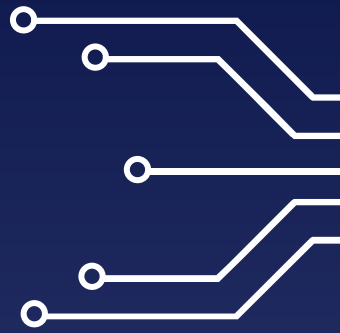
Solution 2 - We make privacy easier for everyone through usable & accessible tools.

** These do not need to be mutually exclusive solutions!*

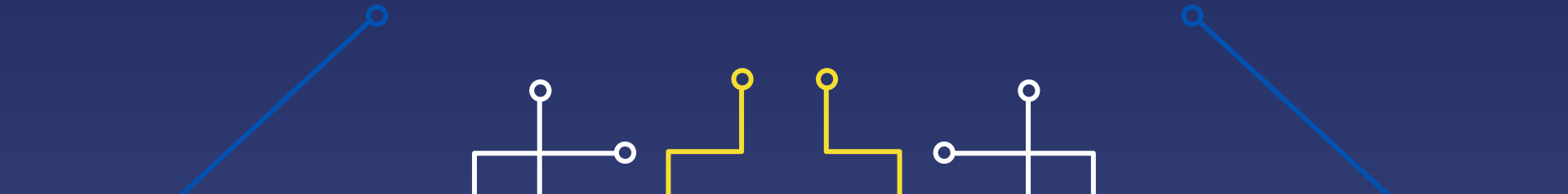


DISCLAIMER





Today I want to demonstrate the projects *(psst. Monero)* that achieve usable privacy, and how the future of privacy for the average person lies in the hands of those developing usable solutions.



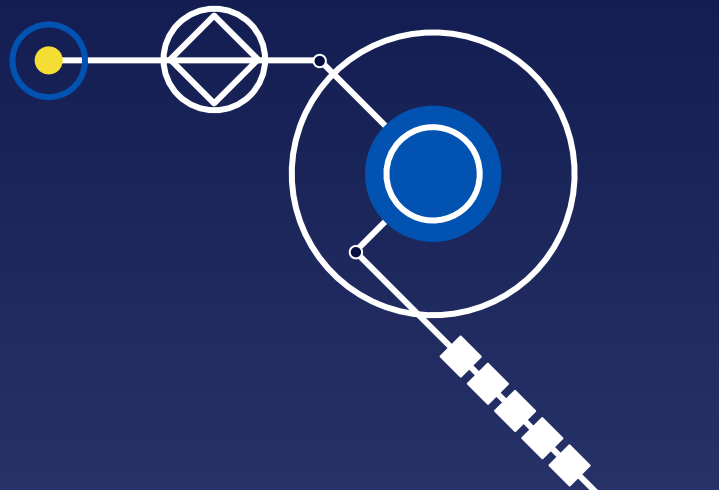
01

THE PATTERN

Many privacy-oriented projects follow harmful patterns.

The Pattern...

- Getting a safe ROM – Requires technical experience to install. Iffy support for apps & features. Still doesn't protect from user error.
- Using Telegram securely – Need to instruct every user to understand and use Secret Chats. *(Doesn't even work on all desktop clients!)*
- Hardening Firefox – Requires technical experience, time, and massive inconvience day-to-day via site breakage.
- Many more, but worst of all...



Bitcoin!

PS. Love you Matt <3

ODELL
@ODELL
Tweets saying bitcoin cannot be stopped get massive engagement but the sad reality is that many individuals are going to get burned due to not understanding the nuances of using bitcoin privately.
9:42 AM · Feb 16, 2022 · Twitter Web App
160 Retweets 25 Quote Tweets 1,334 Likes
Tweet your reply
Reply
ODELL @ODELL · Feb 16
Replying to @ODELL
Bitcoin Privacy
by Matt Odell
21 resources
36 hours 55 minutes
Swan
swanbitcoin.com
Bitcoin Privacy by Matt Odell
You may get overwhelmed at first but do not let that stop you, every small step you make in the right direction helps and at scale helps all ...
12
93
387

Bitcoin Privacy

You may get overwhelmed at first but do not let that stop you, every small step you make in the right direction helps and at scale helps all of us use bitcoin more privately.

Created by **Matt Odell**
@ODELL

Total time
36 hours 55 minutes

0/21 completed

37 Hours

To use Bitcoin privately

0 Hours

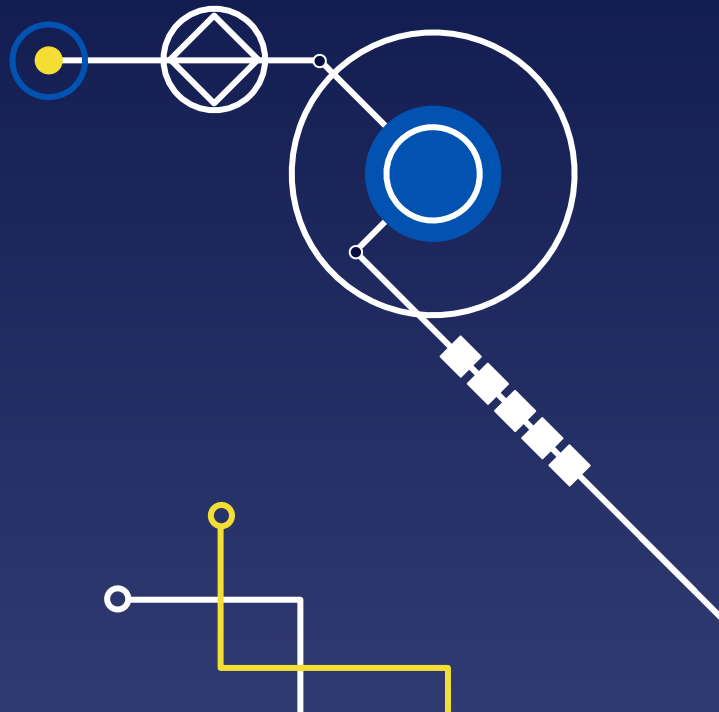
To use Monero privately

"The way of thinking which is the most inappropriate of all is the one which does not see, or worse, simply tolerates, unnecessary difficulty. From there, it is only a small step to the degeneration of cults of collusion which not only condone, but actually cultivate complicatedness."

- Poet Cliff Crego

What needs to change?

- Privacy **MUST** be a default, no matter the user.
- Bitcoin and other projects neglecting default privacy for users are consciously choosing to make privacy a privelege.
- It ideally should be the tool's job, not the user, to coach them through proper privacy use.

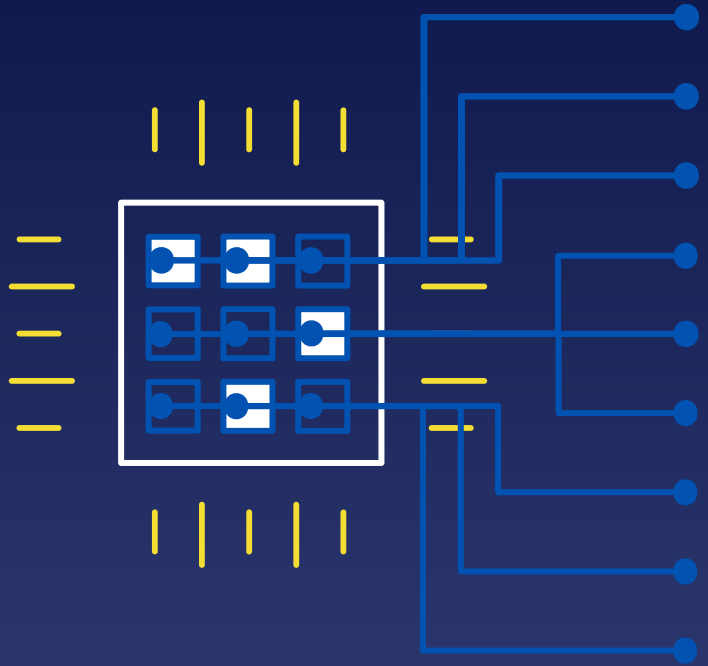


02

PROJECTS THAT BREAK THE PATTERN

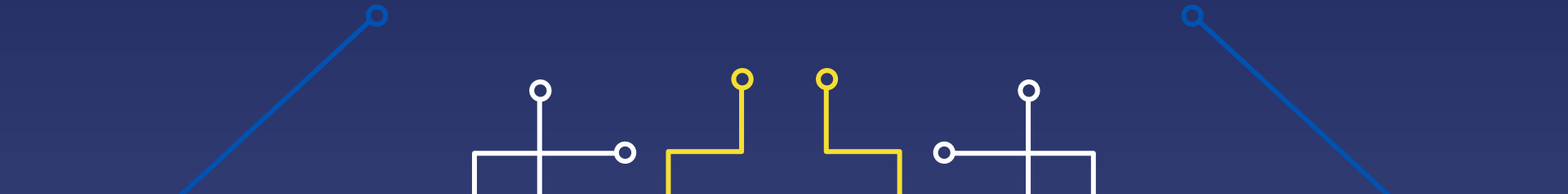
Monero!

More Examples



E2EE Messaging	Signal
E2EE Messaging	Session
Anonymous Web Browsing	TBB
Private Web Browsing	LibreWolf
Safe Notes	Cryptee
Safe File Sharing	OnionShare
Safe(r) Email	ProtonMail
Even Easier Monero	Cake Wallet
Anonymous Messaging	Briar

While these projects achieve a great layer of privacy by default, they are not and can never be perfect. *But why not chase perfection?*

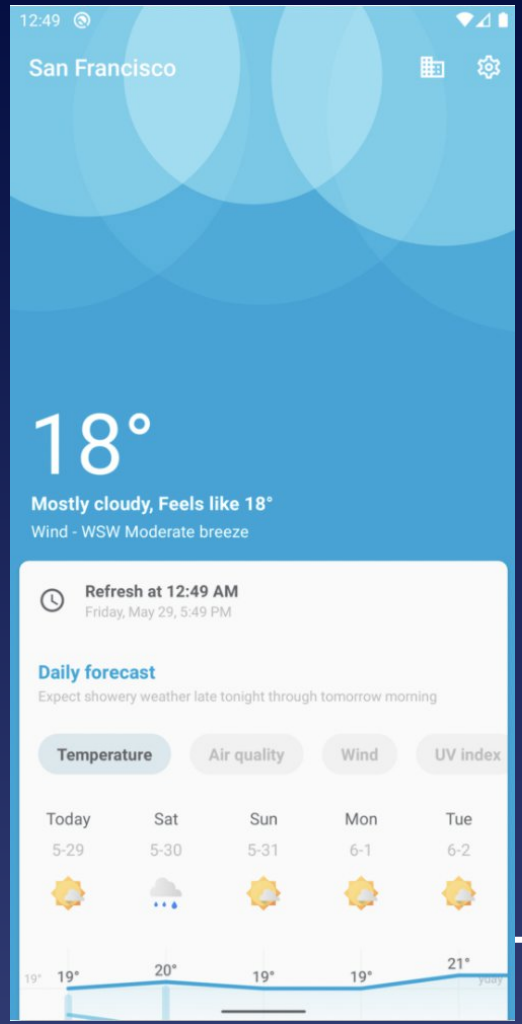


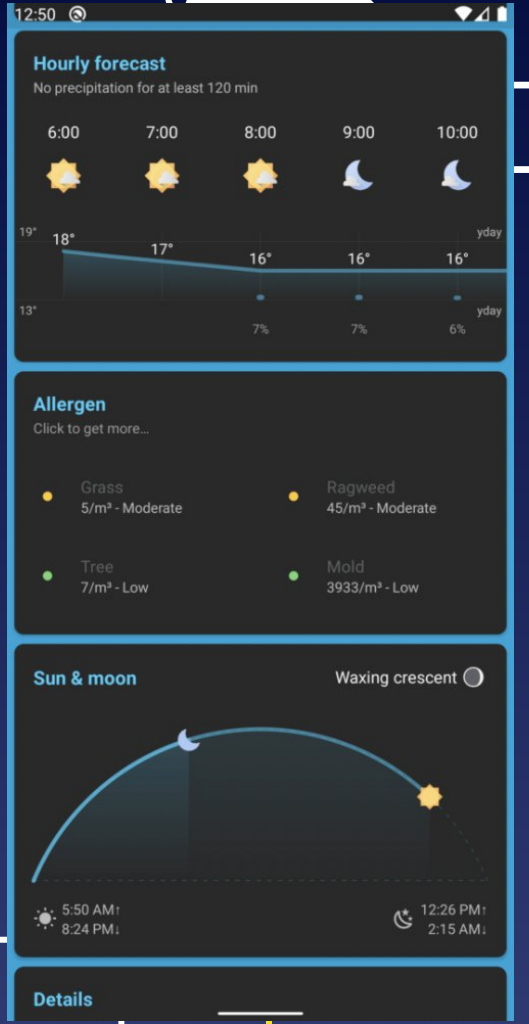
Final Note: Sometimes the improved work is done after-the-fact. *(Ex. LibreWolf, Haveno, Cake Wallet)*

03

THE LARGEST PRIVACY MYTH

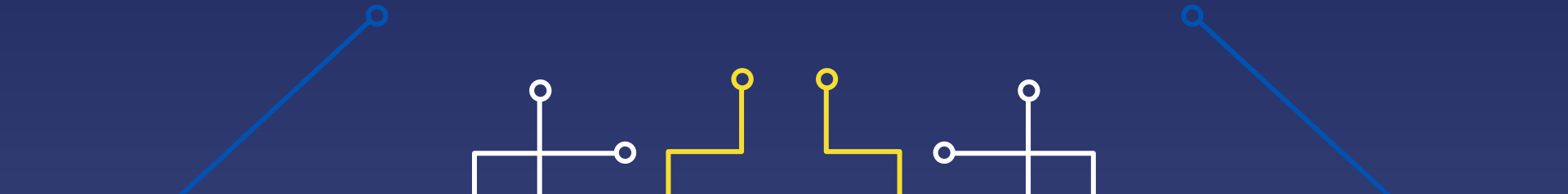
My Skeptical Client





Privacy can be beautiful, simple, easy, and enjoyable for anyone.

Bitcoin vs Monero is a perfect metaphor for many privacy tools today.



04

ACTIONABLE TAKEAWAYS

For Developers

1. Fortunate to even have so many wonderful examples.

2. We need to make privacy tools
as easy, simple, and beautiful
as possible.

People won’t switch to a new platform unless it’s 10x better than the last.

— *Douglas Tuman (Paraphrasing)*

05

ACTIONABLE TAKEAWAYS

For End Users

Be Honest

Embrace the Suck

Praise the Good Things

Let’s build more unicorn tools for users!

THANK YOU!

Contact Me:

WEB	techlore.tech
EMAIL	support@techlore.tech